サプライヤにおける TARA 実施の現実と課題解決へのヒント

2025 年 6 月 27 日に、無償セミナー「自動車サイバーセキュリティセミナーシリーズ Vol.3 ～サプライヤにおける TARA の実施パターンとポイント～」を開催しました。多くの方々にご参加いただき、サプライヤにおける TARA 実施の実情に関する理解も深まる有意義な時間となりました。今回のセミナーでは、サプライヤが入手できる情報によって TARA の実施形態が大きく異なる点に着目し、現場で見られる TARA の典型的な 4 つのパターンを整理。それぞれの特徴と、どのような工夫が必要となるかについてご紹介しました。

表 1. 入力情報によるコンポーネントレベルの TARA 実施パターン

入力情報		コンポーネントTARAの実施パターン			
		①アイテムレベルのTARAの更新	②車両構造に基づくTARA	③コンポーネントの情報に基づくTARA	④コンテキスト外のTARA
アイテム定義	アイテムの構造	あり	あり	なし（情報はコンポーネントと接する部分のみ）	想定
	運用環境情報	あり	あり	なし（情報はコンポーネントと接する部分のみ）	想定
アイテムレベルTARA結果		あり	なし	なし	想定
サイバーセキュリティコンセプト	サイバーセキュリティゴール	あり	なし	なし	想定
	サイバーセキュリティ要件	あり	あり	あり	想定

セミナーの中で明らかになったのは、多くのサプライヤが非常に限られた情報に基づいて TARA を実施している（表 1 パターン③）という現実です。本来 TARA は、OEM のコンセプト段階からサプライヤで設計が具体化された段階、さらに PSIRT 活動までを通じた継続的なリスク管理を支える要であり、十分な情報に基づく分析が望まれます（図 1 ）。しかし、OEM↔サプライヤなど組織を跨いだ情報共有はかなり慎重に行われる傾向が強く、サプライヤは限られた情報に基づいて創意工夫を重ねながら TARA を実施しています。より実効性のある TARA を行うためには、サプライヤは機密情報を適切に取り扱う仕組みが整備されていることを OEM に示した上で、自社製品に関連する範囲の情報の開示を OEM に求めることが重要です。しかしながら、現実問題として情報が理想的な形で入手できない場合、TARA の実施範囲や前提条件、判断基準などを個別に定めて事前に合意することが必要になります。

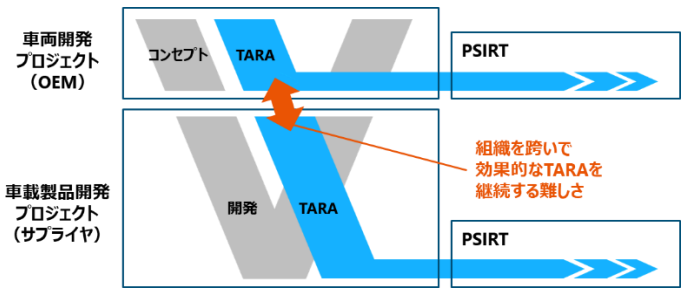

図 1. 製品ライフサイクルにおける TARA の位置づけと難しさ

こうした状況に対応するサービスとして、弊社では「お客様の製品特性に合わせた TARA の仕組みづくり」を支援しています。お客様が得られる情報の内容、粒度や制約条件に応じて、どの範囲で TARA 活動を担うべきか、TARA の前提条件や判断基準の定義をサポートし、現実的かつ合理的なプロセス構築をお手伝いしています。リニューアルされた弊社の Web サイトでは、こうしたコンサルティングサービスについてもご紹介しています。興味をお持ちの方はぜひ一度訪れてみてください。（リンク：業界の相場観や個別ニーズに基づく TARA の仕組みづくり）

また、弊社の Web サイトではサービス紹介の他にも、サイバーセキュリティに関する各国法規などの最新動向や、現場での実装のポイントといった情報も随時更新しています。サイバーセキュリティへの対応を継続して行っていく会社様に有益なヒントをきっと見つけていただけるはずです。無償セミナーや座談会などのイベント情報も随時更新しておりますので、ぜひご覧いただき、「少し話を聞いてみようかな」と思われましたらお気軽にご参加ください。

弊社の Web サイトでは、皆さまの活動の一助となる情報や場をこれからも継続的に発信してまいります。

2025/7/3 大野 貴正